The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:

7/9/2013

SUBJECT:

Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB13-17)

OVERVIEW:

Vulnerabilities have been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. Adobe Flash Player is a multimedia application for multiple platforms.

Successful exploitation could result in an attacker executing code on the vulnerable system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:

- Flash Player 11.7.700.224 and earlier versions for Windows
- Flash Player 11.7.700.225 and earlier versions for Macintosh
- Flash Player 11.2.202.291 and earlier for Linux
- Flash Player 11.1.115.63 and earlier for Android 4.x
- Flash Player 11.1.111.59 and earlier for Android 3.x and 2.x

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: High Home users: **High**

DESCRIPTION:

Adobe Flash Player is prone to vulnerabilities that could allow for remote code execution. The update provided by Adobe resolves heap buffer overflow, integer overflow and memory corruption vulnerabilities that could lead to remote code execution.

Attackers can exploit these issues to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in denial-of-service conditions. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

Update Adobe Flash Player on vulnerable systems immediately after testing.

Users of Adobe Flash Player 11.7.700.224 and earlier versions for Windows should update to Adobe Flash Player 11.8.800.94.

Users of Adobe Flash Player 11.7.700.225 and earlier versions for Macintosh should update to Adobe Flash Player 11.8.800.94.

Users of Adobe Flash Player 11.2.202.291 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.297.

Adobe Flash Player 11.7.700.225 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.8.800.97 for Windows, Macintosh and Linux.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb13-17.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3344

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3345

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3347